

CLAIMS:

- 1 1. A method of converting a first key value for a first communications
2 system to a second key value of a second communications, said method comprising:
3 generating a first intermediate value from at least a portion of said first key
4 value using a first random function;
5 providing at least a portion of said first intermediate value to a second random
6 function to produce a second value;
7 performing an exclusive-or on at least a portion of said first key value and at
8 least a portion of said second value to generate a second intermediate value;
9 providing at least a portion of said second intermediate value to a third
10 random function to produce a third value; and
11 producing at least a first portion of said second key value by performing an
12 exclusive-or on at least a portion of said third value and at least a portion of said first
13 intermediate value.
- 1 2. The method of claim 1 comprising:
2 producing at least a portion of said second intermediate value as at least a
3 second portion of said second key value.
- 1 3. The method of claim 1 wherein said generating comprises the step of:
2 providing said first key value of m bits to a first random function to produce
3 said first intermediate value of n-m bits.
- 1 4. The method of claim 3 wherein said first steps of providing and
2 performing comprise:
3 providing said n-m bit first intermediate value to a second random function to
4 produce an m bit second value; and

5 performing an exclusive-or on said m bit first key value and said m bit second
6 value to generate said second intermediate value with m bits.

1 5. The method of claim 4 wherein said second step of providing and said
2 step of producing comprise:

3 providing said m bit second intermediate value to a third random function to
4 produce a n-m bit third value; and

5 performing an exclusive-or on said n-m bit third value and said n-m bit first
6 intermediate value to generate an n-m bit portion of said second key value.

1 6. The method of claim 5 comprising:

2 providing said m bit second intermediate value as an m bit second portion of
3 said second key value having n bits.

1 7. The method of claim 2 further comprising the steps of:

2 providing said second portion of said second key value to said third random
3 function to produce said third value; and

4 generating said first intermediate value by subjecting said first portion of said
5 second key value to an exclusive-or with said third value.

1 8. The method of claim 7 further comprises:

2 using said second random function to generate said second value from said
3 first intermediate value; and

4 producing at least a portion of said first key by subjecting said second value to
5 an exclusive-or with said second portion of said second key value.

1 9. The method of claim 6 further comprises:

2 providing said m bit first portion of said n bit second key value to said third
3 random function to produce said n-m bit third value; and

4 generating said n-m bit first intermediate value using an exclusive-or of said
5 n-m bit second portion of said n bit second key value with said n-m bit third value.

1 10. The method of claim 9 further comprises:
2 providing said n-m first intermediate value to said second random function to
3 generate an m bit second value; and
4 producing said portion of said first key value having m bits by using an
5 exclusive-or of said m bit first portion of said second key value with said m bit second
6 value.

1 11. A key conversion system for converting a first key value for a first
2 communications system to a second key value of a second communications, said
3 system comprising:
4 processing circuitry adapted to generate a first intermediate value from at least
5 a portion of said first key value using a first random function to provide at least a
6 portion of said first intermediate value to a second random function to produce a
7 second value, to perform an exclusive-or on at least a portion of said first key value
8 and at least a portion of said second value to generate a second intermediate value, to
9 provide at least a portion of said second intermediate value to a third random function
10 to produce a third value and to produce at least a first portion of said second key value
11 by subjecting at least a portion of said third value to an exclusive-or with at least a
12 portion of said first intermediate value.

1 12. The system of claim 11 wherein said processing circuitry further
2 configured to produce at least a portion of said second intermediate value as at least a
3 second portion of said second key value.

1 13. The system of claim 12 wherein said processing circuitry further
2 configured to provide said first key value of m bits to a first random function to
3 produce said first intermediate value of n-m bits.

1 14. The system of claim 13 wherein said processing circuitry further
2 configured to provide said n-m bit first intermediate value to a second random
3 function to produce an m bit second value and to perform an exclusive-or on said m
4 bit first key value and said m bit second value to generate said second intermediate
5 value with m bits.

1 15. The system of claim 14 wherein said processing circuitry configured to
2 provide said m bit second intermediate value to a third random function to produce a
3 n-m bit third value and to perform an exclusive-or on said n-m bit third value and said
4 n-m bit first intermediate value to generate an n-m bit portion of said second key
5 value.

1 16. The system of claim 15 wherein said processing circuitry configured to
2 provide said m bit second intermediate value as an m bit second portion of said
3 second key value having n bits.

1 17. The system of claim 12 wherein said processing circuitry configured to
2 provide said second portion of said second key value to said third random function to
3 produce said third value and to generate said first intermediate value by subjecting
4 said first portion of said second key value to an exclusive-or with said third value.

1 18. The system of claim 17 wherein said processing circuitry configured to
2 use said second random function to generate said second value from said first
3 intermediate value and produce at least a portion of said first key by subjecting said
4 second value to an exclusive-or with said second portion of said second key value.

1 19. The system of claim 16 wherein said processing circuitry configured to
2 provide said m bit first portion of said n bit second key value to said third random
3 function to produce said n-m bit third value and to generate said n-m bit first
4 intermediate value using an exclusive-or of said n-m bit second portion of said n bit
5 second key value with said n-m bit third value.

1 20. The system of claim 19 wherein said processing circuitry is configured
2 to provide said n-m first intermediate value to said second random function to
3 generate an m bit second value and to produce said portion of said first key value
4 having m bits by using an exclusive-or of said m bit first portion of said second key
5 value with said m bit second value.